

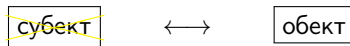
КВАНТОВА ИНФОРМАТИКА

Николай М. Николов

Лекция 3 / 24.10.2022, версия 0

Преговор от предходната лекция

Квантовата теория описва отношението



или, по-конкретно,



без да отстранява субекта / наблюдателя

и да описва обектите “сами по себе си”,

както се прави при класическото описание на природата.

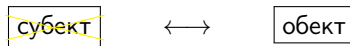
Проблемът: може ли да опишем квантовия свят по класически път е т.нар. “проблем за скритите параметри (hidden variables)”.

Еквивалентно: може ли да симулираме квантовите феномени на класически компютър.

Отговор: да – това е една от целите на квантовата теория.

Преговор от предходната лекция

Квантовата теория описва отношението



или, по-конкретно,



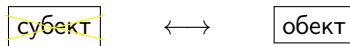
↑
без да отстранява субекта / наблюдателя

Това, което по принцип не може да се постигне, е при една такава симулация да е в сила, че на отделните части на света (напр., на отделни хора) *винаги* ще отговарят отделни части от паметта на класическия компютър, който извършва симулацията.

↑
и да описва обектите “сами по себе си”,
както се прави при класическото описание на природата.

Преговор от предходната лекция

Квантовата теория описва отношението



или, по-конкретно,



без да отстранява субекта / наблюдателя

и да описва обектите “сами по себе си”,

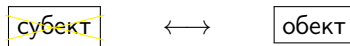
както се прави при класическото описание на природата.

Това следва от т.нар. теорема на Бел, която може да се изказва така: “ако има скрити параметри, то те не са локални”.

Тази теорема е част от раздела по съставни системи.

Преговор от предходната лекция

Квантовата теория описва отношението



или, по-конкретно,



без да отстранява субекта / наблюдателя

и да описва обектите “сами по себе си”,

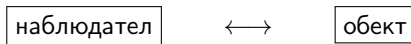
както се прави при класическото описание на природата.

От друга страна, квантовото описание допуска локалност. Тя обаче идва преди всичко от наблюдателната страна.

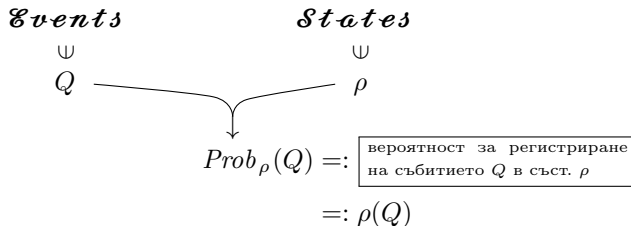
Локалността е особено важна за т.нар. квантова теория на полето (Quantum Field Theory), която поради това също бива наричана “локална квантова физика” (Local Quantum Physics).

Преговор от предходната лекция

Квантовата теория описва отношението



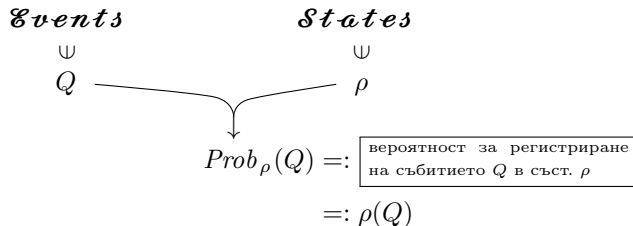
представено от:



Регистрирането на събитие или още казано, установяване на свойство на обект, е “активен процес”. То е нещо като “обичане на дреха върху обекта”, като резултата е “става” / “не става”. При следваща регистрация на събитие, се “облича нова дреха”, което може да заличи старата.

Преговор от предходната лекция

Това са и първите аксиоми:



- Квантова система се задава от: $(\mathcal{E}vents, \mathcal{S}tates, Prob)$.
- Първата аксиома за отделимост
 $=$ състоянията са функции на събитията.
- Втората аксиома за отделимост
 $=$ състоянията *разделят* събитията.

Преговор от предходната лекция

Следващата аксиома може да се изкаже така:

$\mathcal{States}$ е изпъкнало множество в реалното линейно пространство

$$\{f \mid f : \mathcal{Events} \rightarrow \mathbb{R}\}.$$

- При това:
- напомниме, че изпъкналостта на $\mathcal{States}$ означава, че заедно с всеки два него елемента $\rho_1, \rho_2 \in \mathcal{States}$, то съдържа и всяка тяхна изпъкнала комбинация, $\rho = q_1\rho_1 + q_2\rho_2$
(на свой ред, “изпъкнала комбинация” $\Leftrightarrow q_1, q_2 \in [0, 1]$ и $q_1 + q_2 = 1$;
изпъкналите комбинации са точките от свързващата отсечка).
 - Изпъкналите комбинации на състояния наричаме смес на състояния.
Смесването на състояния се интерпретира, като на “квантова” вероятностна смес.
 - Чисто състояние = екстремална точка на $\mathcal{States}$ = такова състояние, което не може да се представи, като нетривиална смес на други състояния.
Смесено състояние = не чисто състояние.

Преговор от предходната лекция

Първи пример: крайни класически системи

Крайна класическа система се строи по едно крайно множество Ω

($\Omega = \{\omega_1, \dots, \omega_n\}$). Тогава:

- $\mathcal{Events} := \mathcal{P}(\Omega) :=$ степенното множество (**power set**) на Ω
(т.е., това е множеството на всички подмножества на Ω);
- $\mathcal{States} := \mathcal{Prob.Func.}(\Omega)$
 $=$ множеството на всички вероятностни разпределения
над Ω ($= \{p : \Omega \rightarrow [0, 1] \mid \sum_{j=1}^n p(\omega_j) = 1\}$)
 $\cong \Delta_{n-1}$ ($(n-1)$ -мерния симплекс)
 $= \{(p_1, \dots, p_n) \in [0, 1]^n \mid p_1 + \dots + p_n = 1\}$.
- Чистите състояния $\longleftrightarrow (p_1, \dots, p_n) = (0, \dots, 0, 1, 0, \dots, 0)$
(в частност, чистите състояния са n на брой).

В ТАЗИ ЛЕЦИЯ ЩЕ ВЪВЕДЕМ

Втори пример: крайни (чисто) квантови системи

Крайна квантова система се строи по $\mathbb{C}^n$ – крайно-мерно, комплексно хилбертово (= унитарно) пространство с размерност n .

- $\mathcal{Events} := \mathcal{L}(\mathbb{C}^n) := \{V \mid V \text{ е линейно подпространство на } \mathbb{C}^n\}$
(това е вече безкрайно множеството);

- $\mathcal{States} := \text{ConvexHull} \{ \rho_\Psi \mid \Psi \in \mathbb{C}^n \text{ е единичен вектор} \},$

$$\text{където } \rho_\Psi(V) := \|\Pi_V \Psi\|^2,$$

а Π_V е ортогоналния проектор върху V

- Чистите състояния ще са тези и само тези, които са от вида ρ_Ψ
(множеството на чистите състояния е също безкрайно).

Аксиомите до тук бяха толкова общи, че допускат не само горните два класа модели, но и много други, които са “безинтересни”.

Една от целите на аксиоматиката е да се въведат такива аксиоми, които освен че са “интуитивни”, също и максимално да стесняват кръга на моделите, по възможност дори, само до тези два класа (и евентуално, “хибриди” между тях).

Преговор по алгебра

Комплексни числа: $\mathbb{C} = \{z = x + iy \mid (x, y) \in \mathbb{R}^2\}$

$$i^2 = -1$$

i – имажинерна единица

$x = \operatorname{Re} z$ – реална част на z

$y = \operatorname{Im} z$ – имажинерна част

$$(x_1 + iy_1)(x_2 + iy_2) = x_1x_2 - y_1y_2 + i(y_1x_2 + x_1y_2)$$

– асоциативно и комутативно умножение.

За $z = x + iy \in \mathbb{C}$: $\bar{z} := x - iy$ – комплексно спрягане,

$$|z| := \sqrt{z\bar{z}} = \sqrt{x^2 + y^2} \text{ – модул на } z.$$

Формула на Ойлер: $e^{i\varphi} = \cos \varphi + i \sin \varphi$

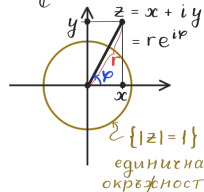
Euler

– общ вид на комплексно число по модул 1.

Полярно разлагане: $z = re^{i\varphi}$,

където $r = |z|$ е модула на z , а φ се нарича аргумент / фаза.

комплексна равнина
 $\mathbb{C}$



Крайно-мерни комплексни хилбертови пространства

(= унитарни пространства)

Определение. Крайно-мерно комплексно хилбертово пространство е крайно-мерно линейно пространство $\mathcal{H}$ над $\mathbb{C}$, снабдено с функция

$$\mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C} : (\Phi, \Psi) \longmapsto \langle \Phi | \Psi \rangle,$$

внимание: наредена двойка число

наречена **скалярно произведение** със свойствата:

- $\langle \alpha\Phi + \beta\Psi | \alpha'\Phi' + \beta'\Psi' \rangle$ (антилинейност-линейност)
 $= \bar{\alpha}\alpha' \langle \Phi | \Phi' \rangle + \bar{\alpha}\beta' \langle \Phi | \Psi' \rangle + \bar{\beta}\alpha' \langle \Psi | \Phi' \rangle + \bar{\beta}\beta' \langle \Psi | \Psi' \rangle,$
- $\langle \Phi | \Psi \rangle = \overline{\langle \Psi | \Phi \rangle}$ (емитова симетрия),
- $\langle \Phi | \Phi \rangle \geq 0$, като $\langle \Phi | \Phi \rangle = 0 \Leftrightarrow \Phi = 0$ (строга положителна дефинитност),

за всеки $\Phi, \Psi, \Phi', \Psi' \in \mathcal{H}$ и $\alpha, \beta, \alpha', \beta' \in \mathbb{C}$.

Елементарната теория на хилбертовите пространства в голяма степен прилича на теорията евклидовите пространства.

(Евклидовите пространства ги наричат също “реални евклидови пространства”).

Например, аналогично на евклидовите пространства въвеждаме понятията: • $\|\Psi\| := \sqrt{\langle \Psi | \Psi \rangle}$ се нарича **норма** (дължина) на вектор Ψ в хилбертово пространство $\mathcal{H}$.

- Ψ е **единичен вектор** $\Leftrightarrow \|\Psi\| = 1$.
- Векторите Ψ и Φ са взаимно **ортогонални** $(\Psi \perp \Phi) \Leftrightarrow \langle \Psi | \Phi \rangle = 0$.
- Базисът $e_1, \dots, e_n$ на $\mathcal{H}$ се нарича **орто-нормиран**, ако се състои от единични вектори, които са взаимно ортогонални.

$$\text{Еквивалентно: } \langle e_j | e_k \rangle = \boxed{\delta_{j,k} := \begin{cases} 1 & \text{при } j = k \\ 0 & \text{при } j \neq k \end{cases}} \leftarrow \begin{cases} \text{делта-символ} \\ \text{на Крьонекер.} \end{cases}$$

Елементарната теория на хилбертовите пространства в голяма степен прилича на теорията евклидовите пространства.

(Евклидовите пространства ги наричат също “реални евклидови пространства”).

Например, аналогично на евклидовите пространства въвеждаме понятията: • Ако $V \subseteq \mathcal{H}$ е линейно подпространство, то

$$V^\perp := \{\Phi \in \mathcal{H} \mid \Phi \perp \Psi \text{ за всяко } \Psi \in V\}$$

наричаме **ортогонално допълнение** на V .

Теорема.

Всеки вектор $\Theta \in \mathcal{H}$ се представя по единствен начин като сума:

$$\Theta = \Psi + \Phi \quad \text{за } \Psi \in V \text{ и } \Phi \in V^\perp.$$

Последното се записва също така: $\mathcal{H} = V \oplus V^\perp$.

Полагането $\Pi_V(\Theta) := \Psi$ определя линеен оператор $\Pi_V : \mathcal{H} \rightarrow \mathcal{H}$, наречен **ортогонален проектор върху V** .

Основен пример на хилбертово пространство:

Това е $\mathbb{C}^n$ снабдено със скаларното произведение:

$$\langle \Psi | \Phi \rangle = \overline{\psi}_1 \phi_1 + \cdots \overline{\psi}_n \phi_n,$$

$$\text{ако } \Psi = (\psi_1, \dots, \psi_n) \in \mathbb{C}^n \text{ и}$$

$$\Phi = (\phi_1, \dots, \phi_n) \in \mathbb{C}^n.$$

Скаларното произведение в орто-нормиран базис придобива вида на скаларното произведение в $\mathbb{C}^n$ и по такъв начин, разглеждането на хилбертовото пространство $\mathbb{C}^n$ е равносилно на задаване на n -мерно хилбертово пространство с *посочен* орто-нормиран базис.

Аксиоми на квантово-логическия подход – част 2

Логическата наредба между събитията

Въвеждаме бинарна релация в множеството на събитията *Events*:
за $P, Q \in \mathcal{Events}$ нека

$P \preceq Q$ се определя чрез условието,
че за всички състояния $\rho, \sigma \in \mathcal{States}$,
от $Prob_{\rho}(P) = 1$ следва, че $Prob_{\rho}(Q) = 1$,
от $Prob_{\sigma}(Q) = 0$ следва, че $Prob_{\sigma}(P) = 0$.

Когато $P \preceq Q$ ще казваме, че

събитието P **се мажорира** от събитието Q .

Синоними:

$Q \succeq P$, “ Q мажорира P ”, “ P се съдържа в Q ”,
“ Q съдържа P ”, “от P следва Q ”, “ Q следва от P ”.

Непосредствени следствия (чисто логически):

(рефлексивност) за всяко събитие P имаме: $P \preceq P$;

(транзитивност) за всеки три събития P , Q и R имаме че:
от $P \preceq Q$ и $Q \preceq R$ следва $P \preceq R$.

Като поредна *аксиома* налагаме следното свойство:

■ (антисиметрия) за всеки две събития P и Q имаме че:
от $P \preceq Q$ и $Q \preceq P$ следва $P = Q$.

Еквивалентно, $P = Q \Leftrightarrow \begin{cases} Prob_{\rho}(P) = 1 \Leftrightarrow Prob_{\rho}(Q) = 1 \quad (\forall \rho), \\ Prob_{\sigma}(P) = 0 \Leftrightarrow Prob_{\sigma}(Q) = 0 \quad (\forall \sigma). \end{cases}$

Издадена с думи горната аксиома гласи, че ако P , респективно, настъпва или не настъпва, тогава и само тогава, когато Q настъпва или не настъпва, то тогава P и Q са едно и също събитие. Новата аксиомата засилва втората аксиома за отделимост, както непосредствено се вижда от еквивалентната формулировка.

И така, свойствата на релацията $\preceq$ са:

(рефлексивност) за всяко събитие P имаме: $P \preceq P$;

(транзитивност) за всеки три събития P , Q и R имаме че:
от $P \preceq Q$ и $Q \preceq R$ следва $P \preceq R$;

(антисиметрия) за всеки две събития P и Q имаме че:
от $P \preceq Q$ и $Q \preceq P$ следва $P = Q$.

По такъв начин, множеството *Events*, снабдено с релацията $\preceq$, се превръща в *частично наредено множество* (partially ordered set = poset), тъй като (нека припомним, че) горните три свойства се явяват дефиниционни за това.

В следствие на допълнителни аксиоми ще получим усилването:

$P \preceq Q$ тогава и само тогава, когато

за всяко състояние $\rho \in \mathbf{States}$: $Prob_{\rho}(P) \leq Prob_{\rho}(Q)$

За класическите системи, когато $\mathcal{Events} = \mathcal{P}(\Omega)$, релацията $\preceq$ е просто релацията на включване на едно подмножество в друго:

$$P \preceq Q \iff P \subseteq Q$$

за всеки $P, Q \subseteq \Omega$ (т.е., $P, Q \in \mathcal{P}(\Omega) = \mathcal{Events}$).

За квантовите системи, когато $\mathcal{Events} = \mathcal{L}(\mathbb{C}^n)$, релацията $\preceq$ е отново релацията на включване, но едно линейно подпространство в друго:

$$V \preceq W \iff V \subseteq W$$

за всеки $V, W \underset{\text{лин.}}{\subseteq} \mathbb{C}^n$ (т.е., $V, W \in \mathcal{L}(\mathbb{C}^n) = \mathcal{Events}$).

Аксиома за нулата и единицата:

в частично нареденото множество на всички събития съществуват *най-голям* *най-малък* елемент.

Последните ще означаваме с **0** (нула) и **1** (единица), съответно.

невъзможното събитие

винаги изпълненото събитие

Написано с формули: за всяко събитие $P \in \mathcal{Events}$ имаме:

$$0 \preceq P \preceq 1.$$

От допълнителните аксиоми по-нататък ще следва, че:

$P = 0$ тогава и само тогава, когато

за всяко състояние $\rho \in \mathcal{States}$: $Prob_{\rho}(P) = 0$.

и също $P = 1$ тогава и само тогава, когато

за всяко състояние $\rho \in \mathcal{States}$: $Prob_{\rho}(P) = 1$.

За класическите системи (когато $\mathcal{Events} = \mathcal{P}(\Omega)$):

$$\mathbf{0} = \emptyset \in \mathcal{P}(\Omega) (= \mathcal{Events}),$$

$$\mathbf{1} = \Omega \in \mathcal{P}(\Omega) (= \mathcal{Events}).$$

За квантовите системи (когато $\mathcal{Events} = \mathcal{L}(\mathbb{C}^n)$):

$$\mathbf{0} = \{0\} \in \mathcal{L}(\mathbb{C}^n) (= \mathcal{Events}),$$

$$\mathbf{1} = \mathbb{C}^n \in \mathcal{L}(\mathbb{C}^n) (= \mathcal{Events}).$$

Логическите операции “и” и “или” за събития

Всяко частично наредено множество допуска формулирането на логическите операции “и” и “или” посредством понятията за *инфимум* (или още, *точна долна граница*) и *супремум* (*точна горна граница*), съответно.

Нашата следваща *аксиома* е, че

в множеството на всички събития съществуват инфимумите и супремумите на произволни подмножества от събития.

Припомняне: ако $(\mathcal{T}, \preceq)$ е едно частично наредено множество и $S \subseteq \mathcal{T}$, то **инфимум** на S се определя като:

$$\wedge S (\equiv \inf S) := a \iff \begin{cases} \forall x \in S : a \preceq x \\ \forall y \in \mathcal{T} : (\forall x \in S : y \preceq x) \Rightarrow y \preceq a. \end{cases}$$

Изказано с думи, a е най-големия елемент в множеството на всички елементи y , които са по-малки от всеки елемент x на S .

Дуално понятие е **супремума**:

$$\vee S (\equiv \sup S) := a \iff \begin{cases} \forall x \in S : x \preceq a \\ \forall y \in \mathcal{T} : (\forall x \in S : x \preceq y) \Rightarrow a \preceq y. \end{cases}$$

Изказано с думи, a е най-малкия елемент в множеството на всички елементи y , които са по-големи от всеки елемент x на S .

Подчертаваме, че елементите $\wedge S$ и $\vee S$ не винаги съществуват.

Доказва се обаче, че ако съществуват $\wedge S$ или $\vee S$, то определенията по-горе ги дефинират еднозначно.

Забележка: Нека отбележим, че ако частично нареденото множество $(\mathcal{T}, \preceq)$ има нула и единица, то

- $\wedge \emptyset = \mathbf{1}, \quad \vee \emptyset = \mathbf{0}, \quad \wedge \mathcal{T} = \mathbf{0}, \quad \vee \mathcal{T} = \mathbf{1}.$
- $\vee S = \wedge \{y \in \mathcal{T} \mid \forall x \in S : x \preceq y\}.$
- $\wedge S = \vee \{y \in \mathcal{T} \mid \forall x \in S : y \preceq x\}.$

В математиката, частично наредени множества, в които произволни, непразни, крайни подмножества от елементи имат супремум и инфимум, се наричат *решетки* (наредбени)(**lattice**).

Ако в решетка съществуват супремумите и инфимумите на произволни подмножества, тогава решетката се нарича *пълна* (**complete lattice**).

По такъв начин, аксиомите формулирани до тук могат да се свият просто до формулировката, че *множеството на събитията **Events** е пълна решетка с нула и единица, спрямо операцията “ $\preceq$ ”, в качеството на частична наредба.*

Особено важен случай е, когато имаме инфимум и супремум на множество от два елемента. За $P, Q \in \mathcal{Events}$ полагаме:

$$\begin{aligned}P \wedge Q \quad (\equiv \quad P \text{ и } Q) &:= \wedge \{P, Q\}, \\P \vee Q \quad (\equiv \quad P \text{ или } Q) &:= \vee \{P, Q\}\end{aligned}$$

и по-нататък ние основно ще използваме означения “ $\wedge$ ” и “ $\vee$ ” за обозначаване на логическите операции “и” и “или” между събитията, съответно.

По-нататък, операциите “ $\wedge$ ” и “ $\vee$ ” ще наричаме също **решетъчни операции**.

“ $\wedge$ ” и “ $\vee$ ” могат да се разглеждат, като бинарни операции..

За класическите системи множеството на събитията, което е степенното множество, е пълна решетка.

В този случай решетъчните операции “ $\wedge$ ” и “ $\vee$ ” съвпадат с теоретико-множествените операции сечение “ $\cap$ ” и обединение “ $\cup$ ”, съответно:

$$P \wedge Q = P \cap Q, \quad P \vee Q = P \cup Q$$

за всеки $P, Q \in \mathcal{Events} = \mathcal{P}(\Omega)$ (класическа система).

Аксиома за отрицанието:

за всяко събитие P съществува събитие Q такова, че Q се случва (наблюдава) тогава и само тогава, когато P не се случва, както и P се случва тогава и само тогава, когато Q не се случва.

Написано с формула това условие изглежда така: за всяко състояние $\rho \in \mathcal{States}$ имаме следните еквивалентности:

$$\begin{aligned} Prob_{\rho}(P) = 1 & \iff Prob_{\rho}(Q) = 0, \\ Prob_{\rho}(P) = 0 & \iff Prob_{\rho}(Q) = 1 \end{aligned}$$

От аксиомата за наредбата следва, че събитието Q е еднозначно определено от събитието P .

Ще казваме, че Q е **отрицание на събитието P** и ще пишем:

$$Q =: P^{\perp} (\equiv \text{не } P).$$

Следствие: $P_1 \preceq P_2 \implies P_2^\perp = P_1^\perp.$

От останалите аксиоми по-нататък ще покажем, че:

$$Prob_\rho(P^\perp) = 1 - Prob_\rho(P)$$

за всички $P \in \mathcal{Events}$ и $\rho \in \mathcal{States}$.

За класическите системи отрицанието е теоретико-множественото допълнение:

$$P^\perp = \Omega \setminus P$$

за всеки $P, Q \in \mathcal{Events} = \mathcal{P}(\Omega)$ (класическа система).

Общи закони на съждителното (пропозиционалното) смятане за събития

$$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R, \quad P \vee (Q \vee R) = (P \vee Q) \vee R,$$

твърдения за асоциативност;

$$P \wedge Q = Q \wedge P, \quad P \vee Q = Q \vee P,$$

твърдения за комутативност;

$$P \vee (P \wedge Q) = P, \quad P \wedge (P \vee Q) = P,$$

твърдения за “поглъщането”;

$$P \wedge P = P = P \vee P,$$

твърдения за идемпотентност;

$$P \wedge Q = P \Leftrightarrow Q \preceq P, \quad P \vee Q = Q \Leftrightarrow P \preceq Q,$$

обратна характеристика на релацията на частична наредба $\preceq$
посредством операциите $\wedge$ или $\vee$;

$$(P^\perp)^\perp = P,$$

идемпотентността на отрицанието;

$$P \vee P^\perp = \mathbf{1}, \quad P \wedge P^\perp = \mathbf{0}, \quad \mathbf{1}^\perp = \mathbf{0},$$

закон за изключеното трето и др.;

$$(P \wedge Q)^\perp = P^\perp \vee Q^\perp, \quad (P \vee Q)^\perp = P^\perp \wedge Q^\perp,$$

законите на де Морган.

(за всеки $P, Q, R \in \mathcal{Events}$).

Това са законите за класическото съждително смятане, от които са изпуснати само законите за *дистрибутивност*:

$$\begin{aligned}P \wedge (Q \vee R) &= (P \wedge Q) \vee (P \wedge R), \\P \vee (Q \wedge R) &= (P \vee Q) \wedge (P \vee R).\end{aligned}$$

В общия случай, това което следва вместо тъждествата за дистрибутивност, са неравенства:

$$\begin{aligned}P \wedge (Q \vee R) &\succcurlyeq (P \wedge Q) \vee (P \wedge R), \\P \vee (Q \wedge R) &\preccurlyeq (P \vee Q) \wedge (P \vee R)\end{aligned}$$

В алгебрата, множество с бинарни операции “ $\wedge$ ” и “ $\vee$ ” и едномесна операция “ $\perp$ ”, в което изпълняват тъждествата от предната страница, се нарича **орто-решетка**.

Така, аксиомите до тук могат на кратко да се изкажат така:

*множеството **Events** на квантовите събития е орто-решетка (спрямо релацията “ $\preccurlyeq$ ” и операциите “ $\wedge$ ” и “ $\vee$ ”).*

Аксиома за орто-модуларност

(закон за орто-модуларност)

ако $P \preceq Q$ тогава $P \vee (P^\perp \wedge Q) = Q$

за всеки две събития $P, Q \in \mathcal{Events}$.

Може да се разглежда, като специален случай на дистрибутивност понеже:

$$P \vee (P^\perp \wedge Q) = (P \vee P^\perp) \wedge (P \wedge Q) = \mathbf{1} \wedge Q = Q.$$

В алгебрата: ... това са **орто-модуларни решетки**.

В една класическа система:

за събития P, Q , ако $P \preceq Q$, то $Q \wedge P^\perp$ е допълнението на P в Q ,
 $Q \setminus P := P^\perp \wedge Q$. Пренесяме това и в общи орто-модуларни решетки.
Така, закона за орто-модуларност приема вида:

ако $P \preceq Q$ тогава $P \vee (Q \setminus P) = Q$.

Състоянията като вероятности върху орто-решетката на събитията

Завършващи аксиоми за състоянията в общите системи:

Всяко състояние $\rho \in \mathcal{States}$ изпълнява свойствата:

адитивност $\rho(Q) = \rho(P) + \rho(Q \setminus P)$, за всеки две събития $P, Q \in \mathcal{Events}$, за които $P \preceq Q$;

нормираност $\rho(1) = 1$.

→ Вероятност върху орто-решетка.

Множеството на всички вероятности върху орто-решетка е изпълнено.

За всяко ненулево събитие $P \in \mathcal{Events}$ съществува състояние $\rho \in \sigma$, в което P настъпва почти сигурно, т.е., $Prob_\rho(P) = 1$.

По-нататък ще покажем, че от аксиомите следва, че $\mathcal{States}$ съвпада с множеството на всички вероятности върху орто-решетката $\mathcal{Events}$.

Така, структуро-определяща е именно орто-решетката на събитията $\mathcal{Events}$

Определение. Елементарно събитие е събитие $P \in \mathcal{Events}$,
такова, че за всяко друго събитие $Q \in \mathcal{Events}$ следва, че:

$$Q \preceq P \implies Q = \mathbf{0} \text{ или } Q = P.$$

В теорията на частично наредените множества с *най-малък елемент* (и в частност, решетките с $\hat{0}$ и $\hat{1}$) горното свойство определя понятието **атом в частично наредено множество**.

Така, *елементарните събития* – това са *атомите на решетката на събитията*.

Аксиома за атомарност:

■ всяко ненулево събитие мажорира поне едно елементарно събитие.

Определение на ниво на събитие.

Нулевото събитие и само то има **ниво нула**. За едно *ненулево* събитие P , казваме че има **крайно ниво**, ако всяка верига

$$\begin{aligned}0 &= P_0 \preceq P_1 \preceq P_2 \preceq \cdots \preceq P_r = P \\ P_0 &\neq P_1 \neq P_2 \neq \cdots \neq P_r\end{aligned}$$

е *крайна* и в множеството на тези вериги има такива с *най-голяма дължина* r .

Числото $r \geq 1$ се нарича **ниво на ненулевото събитие** P .

Ясно е, че *елементарните събития са тези и само тези събития, които са от ниво 1*.

Системата наричаме от **система от крайно ниво** или още **крайна система**, ако *единицата 1 има крайно ниво*.

Тогава нивото на единицата ще наричаме **ранг на системата**.

Аксиома за крайност:

■ Всички системи на квантовата информатика са крайни.

Това е равносилно на твърдението, че всички събития имат крайно ниво.

Едни от най-фундаменталните системи на квантовата информатика са системите от ниво 2: това е **системата на един бит**.

По-нататък в този курс ще покажем, че *в следствие на аксиомите ни, има по същество точно две системи от ниво две: това са класическия и квантовия бит.*

Последния се нарича също **q -бит**

Определение. В едно частично наредено множество $\mathcal{T}$ и два негови елемента $a, b \in \mathcal{T}$ казваме, че

$$\begin{aligned} b \text{ покрива } a, \text{ ако } a \preceq b, a \neq b \text{ и за всеки елемент } c \in \mathcal{T}, \\ a \preceq c \preceq b \implies a = c \text{ или } b = c. \end{aligned}$$

Така, твърдението, че a е атом на частично наредено множество $\mathcal{T}$ с най-малък елемент $0 \in \mathcal{T}$ е равносилно на изказването, че a покрива 0 .

Последната аксиома е известна също, като **закон за покриването**:

Ако P е елементарно събитие, а Q е събитие, такова че $P \wedge Q = 0$, тогава $P \vee Q$ покрива Q .

Еквивалентно, ако P е елементарно събитие, а Q е събитие, такова че $P \wedge Q = 0$, тогава $(P \vee Q) \wedge P^\perp$ е елементарно събитие.

Последната еквивалентност оставяме без доказателство.